

Евдокимов К.Н.,

кандидат юридических наук, доцент
Иркутский юридический институт (филиала)
Университета прокуратуры Российской Федерации

Актуальные вопросы предупреждения киберпреступности в Российской Федерации

Киберпреступность в настоящее время является одной из основных угроз национальной безопасности Российской Федерации, причиняя огромный вред российской экономике.

Так, по экспертным оценкам, ущерб экономике России в 2018 г. от киберпреступлений составил более 1,1 триллионов рублей¹, в 2019 г. – около 2,5 триллионов рублей², в 2020 г. – 3,5 триллионов рублей, а в 2021 г. достиг 7 триллионов рублей³.

При этом основными видами киберпреступлений выступают кражи электронных денежных средств, различные виды мошенничеств, совершенные с использованием информационно-коммуникационных технологий, которые составляют до 80% преступлений в структуре российской киберпреступности. Достаточно часто жертвами киберпреступников становятся банки, финансово-кредитные организации, крупные компании и корпорации. Так, в 2019 г. с банковских счетов физических и юридических лиц было похищено свыше 6, 4 миллиардов рублей⁴.

В январе 2021 г. хакерская группировка MoneyTaker смогла похитить деньги неназванного российского банка с его корсчета в Центробанке на сумму

свыше 500 миллионов рублей, используя уязвимости в приложении «Автоматизированное рабочее место клиента Банка России (АРМ КБР)», что следует из отчета компании Group-IB об угрозах безопасности финансового сектора «Большой куш: угрозы для финансовых организаций» за 1 полугодие 2021 г.⁵

При этом количество киберпреступлений, зарегистрированных в Российской Федерации ежегодно возрастает в арифметической прогрессии. Например, если в 2015 г. в России были зарегистрированы 43816 преступлений, совершенных с помощью компьютерных и информационно-коммуникационных технологий (далее – киберпреступления), то в 2018 г. – 174674, в 2019 г. – 294409, в 2020 г. – 510396, в 2021 г. – 517722⁶. Таким образом, динамика российской киберпреступности показывает тенденцию уверенного роста, с 2015 г. по 2021 г. количество зарегистрированных киберпреступлений увеличилось почти в 12 раз (+11816 %). При этом каждое четвертое зарегистрированное в России преступление совершено с использованием информационно-коммуникационных и компьютерных технологий, т.е. относится к киберпреступности.

¹ Сбербанк прогнозирует ущерб экономике России от киберугроз в 2018 году в 1,1 трлн рублей. URL: <https://www.kommersant.ru/doc/3676752> (дата обращения: 20.01.2022).

² Сбербанк оценил ущерб экономике России от кибератак в 2019 году в 2,5 трлн рублей. URL: <https://www.kommersant.ru/doc/4226302> (дата обращения: 20.01.2022).

³ Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности. URL: <https://tass.ru/ekonomika/8761953> (дата обращения: 20.01.2022).

⁴ Платежное похищение. Мошенники украли миллиарды рублей с банковских счетов россиян. URL: <https://rg.ru/2020/02/19/moshenniki-ukrali-milliardy-rublej-s-bankovskih-schetov-rossiian.html> (дата обращения: 07.05.2021).

⁵ Хакеры похитили деньги российского банка. URL: https://finance.rambler.ru/business/47770827/?utm_content=finance_media&utm_medium=read_more&utm_source=copylink (дата обращения: 20.01.2022).

⁶ Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за 2015-2021 годы // Портал правовой статистики. Генеральная прокуратура Российской Федерации : сайт. URL: <http://crimestat.ru/analytics> (дата обращения: 20.01.2022).

Вместе с тем удельный вес количества уголовных дел о киберпреступлениях, направленных в суд с обвинительным заключением, ежегодно снижается. Так в 2018 г. из 174674 зарегистрированных преступных деяний, совершенных с использованием информационно-коммуникационных и компьютерных технологий, в суд направлены уголовные дела о 36767 преступлениях (21, 05%), в 2019 г. – из 294409 по 57221 деянию (19, 43 %), а в 2020 г. из 510396 выявленных преступлений в суд направили уголовные дела с обвинительными заключениями по 82977 деяниям (16, 26 %), в 2021 г. в суд направлены уголовные дела о 111125 преступлениях из 517722 (21,5 %)¹.

Тем самым, рост на 11816 % с 2015 г. по 2021 г. количества выявленных (зарегистрированных) киберпреступлений показывает, что система профилактики киберпреступности практически не функционирует. Удельный вес деяний, уголовные дела о которых направлены в суд с обвинительным заключением, составляющий 21,5%, иллюстрирует крайне низкую эффективность системы борьбы с киберпреступностью.

С учетом вышеуказанного автор предлагает следующие правовые и организационно-технические меры по предупреждению российской киберпреступности.

Расширить сферу деятельности негосударственных правоохранительных организаций: народных дружин (кибердружин), частных охранных предприятий, частных детективных агентств по выявлению, предупреждению, пресечению киберпреступлений путем обеспечения необходимым программно-аппаратным оборудованием и техническими специалистами, законодательного закрепления полномочий по охране компьютерной информации и информационно-коммуникационных сетей физических и юридических лиц, поиску утраченной компьютерной информации, выявлению и

блокированию противоправного контента в информационно-коммуникационных сетях, включая сеть Интернет.

С этой целью полагаем возможным дополнить Федеральный закон от 02.04.2014 № 44-ФЗ «Об участии граждан в охране общественного порядка» положениями о «кибердружинах» и «кибердружинниках», уравнивая последних по правовому статусу с народными дружинниками, предусмотрев государственную регистрацию «кибердружин» и включение их в региональные реестры общественных объединений правоохранительной направленности. Также расширить содержание ст. 3 Закона РФ от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации», включив в перечень видов охранных и сыскных услуг такие услуги, как «охрана компьютерной информации, находящейся в собственности, во владении, в пользовании, хозяйственном ведении, оперативном управлении или доверительном управлении физических и (или) юридических лиц» и «поиск утраченной гражданами или предприятиями, учреждениями, организациями компьютерной информации».

Ввести обязательное лицензирование деятельности физических и юридических лиц в высокотехнологичных сферах (разработка искусственного интеллекта, производство и распространение компьютерных программ, операционных систем, информационно-коммуникационных сетей, мессенджеров и т.д.), внося соответствующие дополнения в Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», в том числе обязательную, а не добровольную (уведомительную) регистрацию всех созданных в Российской Федерации компьютерных программ и баз данных в Федеральной службе по интеллектуальной собственности (Роспатенте).

¹ Форма федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» за 2015-2021 годы.